IN THE SPECIFICATION

Please replace the paragraph beginning at page 17, line 27, with the following amended paragraph:

It should also be noted that the inventive protocol could be reduced to two messages using the standard Fiat-Shamir technique, e.g., A. Fiat et al., "How to Prove Yourself: Practical Solutions to Identification and Signature Problems," CRYPTO '86 (LNCS 263), pp. 186-194, 1987, ~~th~~ the disclosure of which is incorporated by reference herein, for making proofs non-interactive using a hash function to calculate a challenge, but then a proof of security would require the random oracle assumption.